Digital Signature Working Group
February 20, 2001
Meeting Notes

Meeting Chair: Phil Sibert
philip.sibert@ns.doe.gov
202-586-2541

PARTICIPANTS

DOE - Headquarters
Germantown
Connie German
Nelson Barry (Audio)

Forrestal
Phil Sibert

Argonne National Laboratory
Barry Finkel
Miriam Bretscher

Lawrence Livermore National Laboratory
Larry Medina
Nick Mitschkowetz

Nevada Office
Fred Walden

Oak Ridge Ops Office
Sharon Adams

Oak Ridge - Y-12 Plant
Sara Jordon

ORAU
Patricia Veler

OSTI
Lowell Langford

I. GROUND RULES (CONNIE GERMAN)

The ground rules were given.

II. ADMINISTRATIVE ISSUES (PHIL SIBERT)

Phil discussed the Considerations Document. After a short discussion, Nelson Barry said he would post it in PDF rather than HTML. The latest version is dated September 20th. Should be on the web site (Http://CIO.DOE.GOV/UCSP/CONSID.HTM).

GENERAL DISCUSSION

General discussion on what's new?

Who knows something about applications in the community that are now being used and where we need to be going?

Let's start off with what's new with your site?

Fred Walden, NV - We are just now looking into using digital signatures for our work packages. Environmental Restoration Group came to Records Management saying that with the new packages requiring five to six signatures they are spending a lot of time riding from one site to another trying to get these signatures and it would be a big help if we could get some kind of a digital signature program to help with that problem. We are looking into the Adobe Acrobat add-on for digital signatures. There is a new document that was issued by NARA, a guideline on implementing digital signatures. We are going to be using that to make sure we meet all of the requirements. We have to make sure it uses one of the approved encryption formats. The home page address is http://www.nara.gov/records/policy/gpea.html.

Phil said he was not if the encryption used in Adobe Acrobat is an approved encryption format.

Barry Finkel, CH - Nothing to add.

Nick Mitschkowetz, LLNL - Looking into trying to apply the digital signature PKI infrastructure to move Sigma-level data that is too sensitive to send over the classified network. The issue is, would an infrastructure be available–one for both signatures and for encryption. Looking for a business case driver.

The issue for us is, can we implement an infrastructure that will support those kinds of changes? It would be nice if it was supported at the Headquarters level as a nuclear weapons complex utility across facilities.

Sara Jordon, Y-12–Implementing Entrust PKI in the classified network environment. Our modernization initiative will a require secure method for securing messaging with vendors.

Phil asked if Y-12 was going to require the vendors to purchase their own Entrust? Sara said No. I do not know the network details.

Phil asked if Sara knew about the PKI policy issued by Sharon Shank? Are you considering getting the certificates, setting up your ENTRUST capabilities thru the Headquarters contractor?

Sara said they were not using the Headquarters Entrust. They considered it, but they need classified services. We need to learn how to do it in the unclassified environment. We have a Department wide license for these. They will use ENTRUST if there is software available. Phil said Sara should talk to Sharon Shank about that.

Lowell Langford, OSTI–Do not have a digital signature initiative. He said he is retiring on April 20, 2001. He will let the group know who will replace him at OSTI.

Nelson Barry, HQ–Gave a quick update on the PKI program and where we are with that. We have a number of cross certified CAs in place. Big changes have taken place since we are integrating registration authority's services to the operations offices. Savannah River and Oakland are up. This month Chicago, Oak Ridge, and a few more. This will provide the operations offices with the ability to issue certificates and software for encryption and digital signature services. We are working with the labs, like Argonne and Brookhaven, to provide this service for those sites as well. As far as VPN, we are negotiating with the operations folks here at Headquarters to provide point-to-point VPN services between Headquarters, Brookhaven, and Headquarters in Crystal City. Also, working with the HR and financial folks to integrate the mechanism for deploying digital certificates.

Phil asked Nelson if he could give some more information on the PKI strategy. Nelson said the strategy was sent forth. He understood that it has been signed, and it will be released very shortly. The big thing we are focusing on right now is the unclassified certificate policy, which is near completion. There are a few issues that need to be referred back to the Federal bridge. One issue will be referred back to NIST for some type of guidance or ruling. Hopefully that will be completed in the next two to three weeks and the final draft will be ready for review. We are also working on a service level agreement between the Office of Cyber Security and the Headquarters operations to provide a number of services, one being to help users around the complex who have problems or issues with the Entrust product. Coverage will be from 7:00 a.m. to 9:00 p.m. East Coast Eastern standard time. The hours will cover the time difference between the West coast and the East coast. Waiting to finalize the directory profile. We have an issue that pertains to mapping between X500 and ETN and DNF. We may be able to solve that with E-mail World with the World Top product. We talked about service level agreements with Headquarters. I

was not available to correct the problem and no one else had his password to get into the server. Have you gotten that issue squared away?

Nelson said they are trying to get a Configuration Management Plan that will avoid that type of problem in the future. We have to make sure the service is available. Phil asked if there were backup personnel on call? Nelson said there are high level availability of services in the CP that need to be added to the Configuration Management plan. We are going to be looking for that in the CPS Practice Statement. That issue belongs to the configuration management plan.

Phil said he has been talking about getting someone to head-up the Digital Signature Working Group in the near future, but no one has stepped forward. I am going to have to drop out of it before too long. It will pass over to Sharon Shank. Someone needs to take over as Chair who I can work with for awhile. Phil said he wanted to talk Nelson about this in the near future. He might be a candidate for this job.

Phil asked Barry Finkel if he had a legislative update. Barry said all bills of the previous Congress that were not passed were no longer active and eventually discarded. They are still on the web site, but they are no longer active. Any bill has to be reintroduced by current members of Congress. I checked the web site and found no bill that pertains to the topic at hand. I'm sure there will be some before too long. Nothing on the tabled list at the moment.

The next topic on the agenda is the content of the Consideration document. Phil said the legal portion needs to be updated and made more generic without a reference to pending bills and so forth. Barry Finkel was asked to look at this and see what suggestions he might have on the legislation development portion of legal issues. Phil suggested including only those bills already enacted into law. Barry agreed to do that.

The document Overview is OK.

Nelson Barry will look over the PKI section. Nick M., LLNL, asked if the DOE PKI strategy would include classified/unclassified. Nelson said he would have to talk to Sharon about that.

The Records Section should be updated to at least reference the NARA document. This does need to be updated to some extent. (Connie German, HQ, will currency of FIPS in Considerations document.) We want to redo those.

Does the department wide license for Entrust cover M&O contractor use? Some licenses are available to M&Os. I think we purchased 20 or 25 thousand–14,000 for Feds; 6, 000 for CI personnel; e.g., contractors, CIAC, etc., who pass sensitive date. There are seat licenses available for M&Os. Encryption algorithms used by entrust are approved by NIST. Sharon Shank is the person to talk to about that. The recommendation is to outline your requirements and submit an

Phil asked if anyone would take a look at the Records Management portion of this and see if we need to update it beyond the narrow reference? Fred Walden said he would do that. Phil did present this document to John Gilligan the CIO and to the acting CIOs Nancy Tomford and then Howard Landon, but nothing has been done with it as far as publishing it and making it official. Need to talk to Howard Landon about getting this out as an official document. Have to have it out there for people to look at. Phil didn't think that publishing it will make a whole lot of difference, but it will be an official DOE document. We will continue to work on that.

There are questions about the formatting of the document. Nelson will take a look at that and correct it. Barry Finkel commented that the pictures are readable in PDF, but not in HTML format.

NEXT STEPS

The next meeting is scheduled for March 21st. Should we have the meeting every other month or monthly? It could be done on an as needed basis. Things are moving quickly, which means the Group should meet every month. Would like to close open items by next month and to cover all the areas that have not been touched on that were lagging from the last couple of months. Maybe consider collaborating with the PKI Strategy Group to work out transitions over the next several months.

We are looking for topics and presentations.

Phil said his e-mail address has changed (philip.sibert@ns.doe.gov). Instead of HQ put NS as in national security. The phone number on the agenda is correct for me.

The Considerations document input should be sent to Phil and Connie German by 3/7/01. The latest version of the Considerations document is at
http://cio.doe.gov/ucsp/DigitalSignatures/Considerations62000.pdf

The meeting was then adjourned.

ADDENDUM TO MINUTES

Barry Hudson–SRS did not participate today but sent this update of the WSRC efforts. Our digital signature efforts are limited to the out-of-the-box capabilities of Lotus Notes. Signatures are used in e-mail and forms. For other applications we have embraced an "electronic approval" posture. Our policy now allows the use of any documented electronic process that has some reasonable proof of identity (from passwords to SecurID cards) for electronic approvals.
Some effort to bring up Entrust has begun, but it will be primarily for support of encryption. Long term, we anticipate that the encryption needs will build both a key infrastructure and directory